# APPENDIX A:
# COUNTY OF LOS ANGELES PUBLIC LIBRARY
# BUSINESS AUTOMATION PLAN:
# FISCAL YEAR 2003-2004

Library

COUNTY OF LOS ANGELES PUBLIC LIBRARY

# BUSINESS AUTOMATION PLAN

## Fiscal Year 2003-2004

## February 28, 2003

# *PUBLIC LIBRARY*

## MISSION STATEMENT

The County of Los Angeles Pubic Library is a network of community-focused libraries that meet the informational, educational, and recreational needs of a highly diverse public. We are committed to supporting lifelong learning and knowledge through self-education. Our helpful and expert staff provides information and quality service and programs in a welcoming environment. We offer a broad and relevant collection, and our expanding information networks use current technology. The Public Library is in the business of satisfying the customer's need to know.

## MAJOR PROGRAMS

Public Services

Public Services provides direct public service to customers to meet their informational, educational, cultural, and recreation needs at 84 community and regional libraries and four bookmobiles, and through telephone and mail service from specialized central services. The Public Services program serves customer needs through circulation of books and materials, answering of reference questions, provision of meeting rooms, and specialized programs such as homework centers, children's reading programs, public access to Internet and support to literacy tutoring.

Support Services - Facilities

Support Services - Facilities provides for the general maintenance and expenses for the operation and support of 84 libraries including building maintenance and repair, grounds maintenance, custodial services, trash, disposal, utilities, lease payments, procurement and warehousing of supplies, delivery of books and supplies to libraries, and contracting for services from other county departments and private vendors.

Information Systems

Information Systems provides for the strategic planning, management, operation, and support of computer, data network, telecommunications, office automation and wireless systems including public access to library materials through the integrated library and on-line public access catalog systems and public access computers. This program also acquires, catalogs, processes, and distributes library materials for customer use at community libraries, and secures materials for public use not available in the Public Library through inter-library loans.

Library Materials

Library materials program provides for the purchase and processing of books, periodicals, videotapes, and other items for circulation to the public and for answering reference questions from customers.

Administration

Provides management direction through finance, budget, human resources, cost accounting, city relations, legislative monitoring, capital planning and other support services.

## INFORMATION TECHNOLOGY MISSION

To ensure that the Public Library information systems are aligned with the business needs of the Library and effectively support its mission.

## BUSINESS GOALS

The Public Library considers information technology (IT) a key component of its service plan to address the

information needs of the County's residents. Public services are enhanced through IT. Departmental awareness and executive commitment to information technology are evidenced by the Public Library's mission statement and the fact that the Department has established responsibility for IT at the Assistant Director level.

*1.0 Have a broad and relevant collection.*

- Establish on-line links to other library jurisdictions to enhance and expand the strengths of our collections and improve access to a wide range of information.
- Maintain a fully functioning integrated library system, including Web access to catalogs, library materials acquisition, and use of the system as a platform to access reference databases.

*2.0 Enhance and broaden the quality and delivery of service to youth.*

- Create interactive learning environments to include use of current technology for reference and information for children.

*3.0 Have library service points to meet changing community needs.*

- Provide the public with Internet access to library information and services.
- Ensure that new and expanded library facilities are equipped with appropriate information technology infrastructure needed to provide quality public service.

*4.0 Use appropriate databases, networks, and technologies to support customer service.*

- Initiate planning efforts to replace the Department's obsolete legacy integrated library system which supports core library business operations including the circulation and acquisition of library materials, library catalog, and access to online reference databases.
- Establish links to information systems in Los Angeles County and other library jurisdictions that improve Departmental effectiveness, productivity, and strengthen reference service to the public.
- Ensure computer literate workforce through technology training.
- Implement a knowledge database application to provide enhanced end user support for business software.
- Replace dumb terminals with NT/Windows 2000 workstations to provide a platform for future software enhancements.

Alignment of Department Goals to County Strategic Plan Goals

| Department Business Goal | County Strategic Goal |
|---|---|
| 1.0 Have a broad and relevant collection.<br>2.0 Enhance and broaden the quality and delivery of service to youth<br>3.0 Have library service points to meet changing community needs | Goal One: Service Excellence –<br>Provide the public with easy access to quality information and services that are both beneficial and responsive. |
| 4.0 Use appropriate databases, networks, and technologies to support customer service | Goal Two: Workforce Excellence –<br>Enhance quality and productivity of County workforce.<br><br>Goal Three: Organizational Effectiveness –<br>Ensure that service delivery systems are efficient, effective and goal oriented. |

## PLANNED FISCAL YEAR 2003-2006 I/T STRATEGIES

1.0 Strategic Planning

**Support Business Goal: Use appropriate databases, network, and technologies to support customer service.**

As instructed by the Board and the CAO, the Public Library is updating its Strategic Plan in conjunction with the County's new Five Year Strategic Plan. This revised strategic plan will consider how to develop financing sources, and revise our service delivery model to ensure the best possible programs and services to children, adults, and our communities. Information technology is a key component of public library service. The Department has formed a working group as part of the its strategic planning process to study the use of modern technology to enhance service to the public and improve organizational effectiveness.

2.0 Library Technology Infrastructure

**Supports Business Goal: Use appropriate databases, networks, and technologies to support customer service.**

During the next three years the Department will complete the information technology and telecommunications infrastructure planning required to support the development for several new and replacement library facilities in accordance with County Network Standards. The Department is also considering the feasibility of wireless technology.

3.0 Integrated Library System Replacement Project

**Supports Business Goal: Use appropriate databases, networks, and technologies to support customer service.**

The Library needs to replace the existing integrated library system, with a new system with graphical interfaces which provides increased functionality for customers and staff. The Library will initiate planning efforts to replace the legacy system, which provides for the registration of library customers, circulation and acquisition of library materials, catalog of library material items and related inventory controls, fines and fees accounting, and customer-placed requests processing. The system also serves as platform to access a variety of online reference databases. This system was implemented in 1988 and has undergone several upgrades over time, but is nearing the end of its useful life. The project will cost an estimated $6.1 million, and will take several years to complete. Funding is included in the Department's Official Budget request.

Project activities include replacement of 329 dumb terminals and 771 outdated workstations with Windows2000 workstations, identifying critical functionality priorities for the new system, developing the project plan, identifying resources (staffing, funding, etc.) to accomplish the project, creating system requirements and other documents for the purchasing process, evaluating bids, contract negotiations, developing a detailed implementation plan, updating and quality control on existing data files to ensure integrity and consistency of data before conversion, data conversion, staff training, system implementation and acceptance testing.

The new system will meet County goals and IT strategic directions for Web-enabled public access to County data and services.

4.0 Computer Replacements

**Supports Business Goal: Use appropriate databases, networks, and technologies to support customer service.**

Replacement of outdated business and public access computers is essential for providing the public with the tools needed to access information in electronic formats and maintenance of business operations. Limited funding of $50,000 is included in the Public Library FY 2003-2004 base budget request. Funding of $579,000 to replace outdated computers is included in the Department's FY 2003-2004 official budget request.

5.0 Library Material Security System Replacements

**Supports Business Goal: Use appropriate databases, networks, and technologies to support customer service.**

Replacement of outdated library material security systems is required to prevent the theft of library materials in newer formats such as CDs and DVDs. The estimated cost for this project is $306,000 and will take approximately 3 years to complete. Funding of $175,000 is included in the Department's FY 2003-2004 base budget request.

6.0 Circulation and Reference Desk Replacements

**Supports Business Goal: Use appropriate databases, networks, and technologies to support customer service.**

Replacement of existing circulation and reference desks, most of which are over 30 years old, with furniture that is designed to incorporate new technology. The estimated cost for this project is $2,710,000. Funding of $150,000 is included in the Department's FY 2003-2004 base budget and the balance is included in the official budget request.

7.0 E-mail Standardization

**Supports Business Goal: Use appropriate databases, networks, and technologies to support customer service.**

Currently, the Department is required to maintain two separate and incompatible e-mail programs since some staff only have access to terminals which will not support GroupWise. A project is in progress to replace 200 remaining staff terminals with computers to allow operation of a single e-mail system. However, sufficient funding has not been identified to fund the total replacement of the terminals. This will improve business communications and enable document sharing and file transfer capability which is not available with the existing terminal based e-mail application. Funding to complete this project is included in the official budget request.

8.0 Provide Effective Maintenance and Support for Existing Applications

**Supports Business Goal: Use appropriate databases, networks, and technologies to support customer service.**

Providing effective and efficient maintenance and support for existing IT applications is a major focus of the Department's IT team. During FY 2001-2002 the Department implemented the use of Service Center software to track end user support requests. In FY 2003-2004 the Department will enhance end user support through the addition of a technical and application support knowledge database. The Department also plans to automate the trouble-ticket reporting process by providing

a Web-enabled application which will allow end users to create online problem reports and status tracking.

In order to improve service to both internal customers and the public, the Department plans to reorganize its end user support by consolidating the Integrated Library System and PC Support help desk functions. Planning efforts are underway to implement this reorganization in conjunction with the Department's strategic planning process.

9.0 Internet/Intranet Applications Development

**Supports Business Goal: Use appropriate databases, networks, and technologies to support customer service.**

This project supports the County's strategic plan to deliver services via the Intranet through the creation of Web-enabled Intranet applications to support internal operations by providing online access to policy and procedures manuals, enhanced readers advisory and information services (reference applications), and office forms.

The Department will embark on a project to enhance the existing County Library website. This project will review the information and services available on the existing web site, and revise many of them to streamline and simplify access by the public. The Children's Services pages will be modified to provide improved access to quality online sources evaluated by Library staff and the Teen section will be enhanced. Better methods to present the Library calendar of events will be explored, to enable customers to more easily find library programs of interest to them in their local community. Also, more sections of the web site will be translated into Spanish, and the Library will explore possibilities for adding community history sections for additional library service areas. The library will continue to explore effective means to provide our customers with additional on-line resources to meet their informational needs, both within the library buildings and through remote access.

10.0 Public Access Computer Connectivity

**Supports Business Goal: Use appropriate databases, network, and technologies to support customer service.**

New library facilities are being planned to explore the feasibility of providing Internet access for customer-owned laptop computers utilizing both wired and wireless technology.

11.0 Public Access Internet Program

**Supports Business Goal: Use appropriate databases, network, and technologies to support customer service.**

The Public Library has been providing computers for the public to access the Internet since FY 1998-1999. Since the inception of this program there has been a 354% increase in Internet usage by library customers. In addition to providing Internet access to meet the public's general needs for information and self-education, the computers located at all County libraries provide convenient locations for the public to access online information on County programs and services. In order to meet increased business demands the Department requires $705,000 to purchase an additional 252 public access computers. Funding for this request is included in the Department's Official Budget Request.

12.0 Software Migration to County Standards

**Supports Business Goal: Use appropriate databases, networks, and technologies to**

**support customer service.**

In keeping with the County's strategic technology plan the Public Library is studying plans to migrate the Department's business networks from Novell NetWare to Windows NT and convert the standard business software currently in use to the Microsoft Office suite.

Migration plans from Novell NetWare to Windows NT are pending the outcome of the County's Active Directory plans.

The full Microsoft Office Suite and Corel Office Suite are currently being installed on the Department's computers. However, WordPerfect is the only program being used in the Corel Suite because of its enhanced editing features.

Internet Explorer and Netscape are installed on public access and staff computers in order to meet public demand and allow Library staff the ability to provide support to the public. In addition, installation of both browsers is needed for viewing Web pages that are designed for a specific browser.

Due to the recent security attacks on the Microsoft Exchange system, the plan to migrate from GroupWise email to Exchange continues to be evaluated by the Department. Because Microsoft has implemented a number of Visual Basic hooks to Exchange that permit hackers and vandals to create viruses that cause extensive damage, Exchange systems experience significantly greater damage than GroupWise systems. GroupWise does not have Visual Basic hooks which makes it far more difficult to create viruses that cause extensive damage. In addition, GroupWise implements a far more secure address book than Exchange. It is fully encrypted and has a unique API. As a result, even if a virus does affect a GroupWise user, it would not be propagated to additional users and cause widespread damage as it would in an Exchange system and downtime is minimal.

## ENTERPRISE ALIGNMENT

### *GOAL ONE: CONDUCT COUNTY GOVERNMENT ELECTRONICALLY*

- The Integrated Library System (ILS) centrally processes approximately 15 million circulation transactions annually received from the County's 84 community libraries and one online bookmobile.

- During FY 2002-2003 the Public Library will replace 230 dumb terminals with Windows2000 workstations to provide a platform for future software enhancements. During 2003-2004 approximately 200 additional terminals will be replaced with computers.

- The Department has implemented a centralized web-enabled photo identification system to allow the issuance of employee identification cards at Library headquarters and the five regional administrative office sites.

- The Public Library's comprehensive Web site provides the public with Internet access to a catalog of over 7 million items and library services.

- The Public Library is participating in the County's electronic commerce efforts by offering fee-based reference services over the Internet.

- The Public Library has implemented a wide area Novell network that links Department headquarters with 7 remote administrative sites. The network allows for collaborative work processing.

- The Public Library currently has 87 facilities equipped with Category 5 cabling, data network, and telecommunications equipment in conformance with County standards.

- The Acquisitions system provides for budget tracking and on-line issuance of purchase orders to vendors for library books and materials

- The Public Library's comprehensive Web site provides the public with 24/7 access to live, assisted reference help.

- The Public Library has created a County-wide informational and interactive Web site for the County's celebration of Cesar Chavez Week. The Library will continue to develop this site and maintain it on an ongoing basis.

- Electronic mail is used to communicate among the Department's 87 facilities, between County Departments, and with other library jurisdictions. Enhanced tools including calendaring and document sharing are available to administrative and supervisory staff at 86 facilities and will be expanded to remaining line staff as funding permits.

- The Document and Information Services Center (DISC) provides centralized access to abstracts and full text copies of magazines, newspaper articles, plays, poetry, essays, and short stories to the public for a minor fee. The center utilizes a Novell network, four high capacity CD-ROM jukeboxes and a fax image server to distribute the information to each of the County's 84 community libraries.

- The Public Library provides a customer-placed request system that allows customers to place requests for library materials through the Internet.

- The Public Library developed an Intranet to allow Web-enabled applications to facilitate access to reference databases and other Library information. The result is improved customer service and quicker on-line access to policy and procedure manuals and routine forms which reduces printing and distribution costs.

***GOAL TWO: PROVIDE SECURED ACCESS TO ELECTRONIC APPLICATIONS***

- In FY 2002-2003 the Public Library migrated to ISD as its Internet service provider, and installed patron authentication software, which enabled authenticated access to vendor databases and on-line resources for Public Library customers. This network reconfiguration allows library staff secure access to County intranet resources. In FY 2003-2004 Public Library will implement secure remote access to administrative systems and e-mail.

***GOAL THREE: UTILIZE ENTERPRISE SOLUTIONS TO MEET COMMON NEEDS***

- The Public Library will utilize ISD's County-wide network infrastructure for data communications. This provides the infrastructure required to support the development of Internet/Intranet applications that would be available at 87 Department facilities, efficient management of Web-based applications for the public, and enhanced communications between community libraries and other County departments. The Public Library has adopted the Z39.50 protocol which allows the Department to share library catalogs with other library jurisdictions.

- Service Center

The Public Library has implemented the Service Center help desk software program to automate the process of recording and tracking IT help calls.

- The Public Library in conjunction with Parks and Recreation Department and ISD has implemented an integrated Web-enabled Internet Management System for public access computers that provides for online computer reservations, filtered Internet access for minors, session control and print management. This system is scaleable can be utilized by any County department that plans to provide public access Internet computers. Initial funding for this project was provided by the Information Technology Infrastructure Fund.

- The Public Library takes advantage of the County's master purchase agreements for the acquisition of hardware, software, and technology services. In addition, the Public Library collaborates with other County Departments and agencies to obtain additional volume discounts.

***GOAL FOUR: IMPROVE THE IT SKILLS OF THE COUNTY WORKFORCE***

- The Public Library is committed to developing the technology competence of both line and IT staff. Commercial vendors and in-house trainers are utilized to present training on core business applications, Internet search techniques, office applications, and technology support issues to ensure a well prepared staff. In addition, a Technology Training Center has been established to provide hands-on classes in a proper environment. A computer-based system is utilized to track employee training.

**FY 2003-2004 IT STAFFING**

The Public Library faces unique IT challenges in serving a geographically diverse organization of 87 facilities located across a 3,000 square mile service area. The Public Library currently operates a 24 x 7 data center that supports a network of over 565 terminals, 535 Windows NT/2000 workstations, over 1,000 staff and public access computers, multiple servers and local area networks connected via a wide area network. In addition to standard business computers, the Public Library is one of the few departments that provide public access computers.

Over the past three years the Department has added over 500 computers and an additional 231 computers will be installed in FY 2003-2004. In order meet increased workload and reduce backlogs the Public Library's FY 2003-2004 budget request includes funding for an existing ordinance Data Systems Analyst I (1.0) position. This position will used to conduct systems analysis and design, routine network maintenance, system configuration, and end user support.

**FY 2003-2004 INFORMATION TECHNOLOGY PROJECTS**

The Public Library will begin efforts on new projects subject to available funding. Project profile reports are attached.

1.0 Integrated Library System Replacement Project

2.0 Library Materials Security System Replacement Project

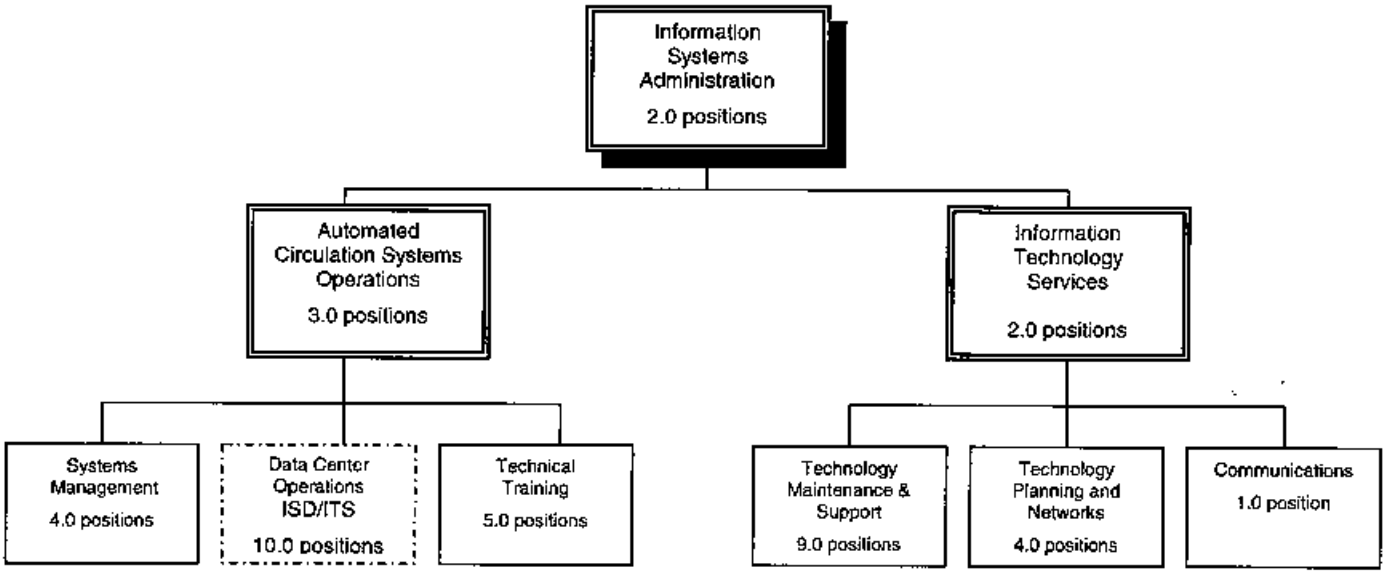
3.0 Library Website Redesign

## I/T ORGANIZATION ASSESSMENT

### Organizational Structure

The Public Library provides library service for the public through a network of 84 community libraries and 4 bookmobiles for 51 cities and the unincorporated area. The Department is organized into four major organization units: Executive Office, Public Services, Finance and Planning, and Information Systems. The Public Library's information technology function is managed by Information Systems. Information Systems has 30 positions and is organized into three organizational units: Information Systems Administration, Automated Circulation Systems Operations, and Information Technology Services. The department operates a 7-day/24 hour data center and supports approximately 565 terminals, 1,735 computers, and multiple local area networks. Wide area network and data center operations support is provided by the Internal Services Department.

**Public Library**
**Information Systems**




### Information Systems Administration

This executive level unit is responsible for overall management of the Department's IT resources, including IT strategic planning, technology development for new facilities, budgeting, management of the Automated Circulation System Operations and Information Systems Sections, data security, technology acquisitions, and coordination with senior managers, other County departments, and outside agencies for program planning and IT decision-making.

### Automated Circulation System Operations

The Automated Circulation System Operations Section manages the Department's mission critical library circulation, acquisitions, and library catalog system, data center operations, wide area network and Internet services, and technology training for mid-range systems applications. This section also participates in the Public Library's overall budget planning and management process for technology, conducts cost/benefit

studies for technology projects and participates in the Department's IT strategic planning process and data security program.

- Systems Management

  The Systems Management unit tests and configures the application and network software to meet the needs of community libraries, Public Service's management and Technical Services, provides standard and customized system reports and help desk support to library staff, determines hardware configurations for terminals, computers, and peripheral equipment used with the system, and coordinates the provision of Internet service. The unit also configures and provides Help Desk support on the Internet Management software.

- Technical Training

  The Technical Training unit provides training for all levels of Library staff on the functions and modules of the Integrated Library System (including circulation, catalog, and acquisitions software) and on the Internet Management software. The unit also drafts system related procedures and manual sections, and provides help desk support to staff.

- Data Center Operations

  The Data Center Operations unit, which is staffed by contract ISD personnel, manages the operation of the Department's mid-range computing data center on a 24 hour, 7-day basis and provides field support for network and terminal equipment. This unit receives direction from the ACS Section Manager and works closely with the Systems Management unit.

**Information Technology Services**

The Information Technology Services Section provides end user and public access computing support, application and Intranet development, design and support of local area networks, and telecommunications management. This section also participates in the Public Library's overall budget planning and management process for technology, conducts cost/benefit studies for technology projects and participates in the Department's IT strategic planning process and data security program.

- Technology Maintenance and Support

  The Technology Maintenance and Support unit provides hardware and software maintenance, system configuration, help desk, and technical support for the Department's public access and business computer systems.

- Technology Planning and Networks

  The Technology Planning and Networks unit is responsible for the planning, design, research, development, implementation and maintenance of Novell based Local Area Network (LAN) and Wide Area Network (WAN) systems, systems analysis and design, micro/mainframe integration and application development.

- Communications

  The Communications unit has department-wide responsibility for planning, and coordinating the design, implementation and maintenance of premises systems wiring, telephone systems and wireless communications. This unit also conducts cost/benefit studies for new systems or modifications to existing systems and participates in the management of the Department's telecommunications budget.

**Organizational Assessment**

The Public Library considers information technology (IT) a key component of its service plan to address the information needs of the County's residents. Public services are augmented through IT. Information Systems provides a comprehensive information technology team, which provides support for over 1,600 staff plus public access computer users located at 87 facilities located throughout Los Angeles County. The Department has an integrated approach to support of its on-line public access, circulation, and catalog system, network infrastructure, LAN/WAN implementation, web-development and hosting, e-commerce, and business systems which utilizes a combination of in-house staff and outsourcing.

This rapidly changing IT environment presents significant challenges for the Department in retrofitting aging facilities with current technology infrastructure, development of new skill sets for community library and IT staff, and managing the support for a constantly increasing base of computers and new applications. To help meet this demand the Department has obtained grants for information technology infrastructure and public access computers. However, there are still significant unmet needs for IT, most notably, the need to replace the Department's Integrated Library System, replacement of outdated staff and public access computers, and additional technical support staff.

**Strengths**

- Departmental awareness and executive commitment to information technology is evidenced by the Public Library's mission statement and IT budget which represents approximately 9% of available resources. The Public Library recognizes the importance of information technology and has placed responsibility for IT management at the Assistant Director level.

- The Department has centralized the management of Information Technology in one branch which improves project coordination and organizational effectiveness.

- IT staff are knowledgeable in both hardware and software support. The ACS Help Desk provides prompt assistance for staff on the mission critical Integrated Library System and on the Internet management software. Hardware/network assistance is provided during all hours that libraries are open to the public (7 days) and software assistance is provided 6 days per week. The Information Technology Services Help Desk provides computer support for staff during business hours on a 5-day basis.

- Outsourcing is a key element of the Department's IT strategy. Currently, the Public Library contracts for the Integrated Library System software and support, Internet access, Web hosting and development, DEC terminal maintenance, data center operations (ISD/ITS), and additional technical support staff for special projects such as high-volume workstation deployments and systems development.

- The Public Library has installed help desk software to automate the process of recording and tracking IT help calls.

### Weaknesses

- The Department is understaffed to support current and future technology requirements. However, limited funding prevents the Department from adjusting the number of IT positions to match the workload.

- Recruitment for IT staff is difficult. Lack of updated class specifications for the IT series, compensation that is adequate to keep pace with the industry trends, and lack of a coordinated Countywide system to schedule frequent examinations for IT positions have hindered the County's ability to recruit and retain IT staff. The Department is actively participating in the interdepartmental working group to develop the new class specifications for the IT series.

## Security Assessment

The Public Library has increased efforts to improve security for information technology resources and data as part of its business continuity planning.

### Strengths

- The Public Library has assembled a Departmental Computer Emergency Response Team (DCERT) and has designated a Departmental Computer Information Security Officer (DCISO) in accordance with County Guidelines.

- The Department actively participates on the Information Security Steering Committee (ISSC)

- All critical Departmental applications require user name and password challenges for logon.

- All servers are located in locked rooms with access controlled by a card entry system.

- Public access computers and peripherals are secured with security cables and padlocks to prevent theft.

- The Public Library is presently developing a strategy for providing remote access to business applications using Secure ID Cards.

- The Department's 24/7 Data Center is equipped with a 75 KVA Uniterruptible Power Supply, emergency generator, three dedicated air conditioning units, and a Halon fire protection system. In addition, daily and weekly backup tapes for the mission critical Intergrated Library System are stored with an offsite data storage vendor.

### Weaknesses

- Budget constraints prohibit the utilization of hot or cold sites for business continuity purposes.

- Dedicated locked rooms or closets for network and telecommunications equipment are not available at many of the Department's 87 facilities.

- Staffing constraints and workload prevent the Department's participation on several of the County's data security committees.

- The Department's data center is not currently located in a seismic resistant structure, however the Public Library plans to relocate to the County's new consolidated data center upon completion.

**Applications Assessment**

The Public Library's computer applications support the Department's mission to meet the informational and educational needs of a diverse public and the County's goal to conduct County business electronically. Public access computers located at all County libraries provide customers with access to local, state, and federal government information over the Internet, on-line reference databases, a variety of self-education programs, and personal productivity software.

**Strengths**

- FYI – e-Commerce

  The Public Library's For Your Information (FYI) e-Commerce application provides the public with the ability to order fee-based reference services over the Internet. This application is current and no further development is required. However, the Department plans to assess the advantages of migrating from the current platform to the Countywide solution currently under development.

- Web-enabled Library Catalog

  A Web-based version of the library catalog of over 7 million items, access to reference databases and links to educational and reference site is available through computers at each community library and over the Internet. This application is updated on a regular basis. In addition, the Department's library catalog is accessible by other library agencies that utilize the Z39.50 protocol.

- Training Management System

  The Department has implemented a new system to track and monitor staff training which utilizes Peopleware Pro software. The new system provides human resources staff with the necessary tools to monitor training requirements and utilization for each staff member and provides enhanced reporting capability.

- Photo ID System

  The Department has implemented a centralized web-enabled photo identification system to allow the issuance of employee identification cards at Library headquarters and the five regional administrative office sites.

### Weaknesses

- Integrated Library System

  The integrated library system software, which is licensed from SIRSI, provides the library functionality to register borrowers, circulate items to the public, provide the on-line library catalog, and to track the acquisition of library materials. The system is primarily uses a text-based interface. The vendor is replacing the older software with a new Windows-based client and a new server. The Department needs to migrate to a new integrated library system to provide staff with increase functionality and a graphical user interface, and to provide customers with enhanced functionality on the Web catalog. The Department plans to replace the terminals with Windows 2000 PCs, and to replace the servers and system software provided that funding can be found for this conversion effort.

- E-mail

  Currently the Department is required to support separate and incompatible e-mail systems due to and the fact that there are an insufficient number of staff computers. However sufficient funding has not yet been identified to fund the total replacement of staff terminals with computers.

- Inventory Control System

  The Public Library utilizes a Microsoft Access database for inventory control purposes. This system is outdated and does not meet current and future requirements. The Department plans to evaluate the use of Asset Center software as a possible replacement for the existing application.

- ACC-PAC

  The Department's warehousing management and supply system is outdated and needs replacement. In addition, the software manufacturer has ceased providing maintenance updates for the system. The Public Library plans to explore the feasibility of replacing the current system with a Web-enabled system that would provide on-line access for staff via the Intranet.

## Technology Training Assessment

The Department is committed to developing a computer literate workforce and improving the skills of our IT staff.

### Strengths

- A computer-training lab has been established at Department Headquarters which provides hands-on training classes on library operations software, business applications, and the Internet. Training is conducted by a combination of library staff and contract trainers.

- The Department takes advantage of office application software training provided for Local 660 members through Comp-USA.

- Public Services staff have developed customized courses for reference staff on Internet searching techniques.

**Weaknesses**

- Fiscal constraints have required the Department to reduce the funding available for technology training in FY 2003-2004.

**Infrastructure Assessment**

**Strengths**

- The Department completed a multi-year program to replace outdated Category 3 data cabling with Category 5 cabling and install digital data network and upgrade telecommunications systems install at 87 Department facilities in order to increase network performance and comply with County standards.

- The Department switched to ISD as the Internet provider in 2002/2003, which provides high speed Internet access required for Department operations at 86 locations.

- Cisco switches have been installed at 86 Library locations, which provide separate VLANs for staff and public devices to enhance data security and allow staff access to secure County resources.

**Weaknesses**

- The Public Library lacks funding to replace over 300 outdated terminals with computers. Budget constraints will require the completion of this project to be spread over a multi-year period.

- Existing circulation and reference desks are unable to accommodate new technology requirements for computers, data cabling, and expanded electrical and will require replacement. Funding constraints will require this program to extend over several years.

**TELECOMMUNICATION AND NETWORKING INITIATIVES**

Data

As the Department continues to expand the number of public access and staff computers, some additional load will be placed on the network. We plan to add an additional 231 public access and staff computers during FY 2003-2004.

Voice

The Department will explore the feasibility of VOIP systems for the new East Los Angeles Library scheduled to open in FY 2003-2004.

Video

The Department is exploring the feasibility of video conferencing and video streaming systems, however, we have no implementation plans for FY 2002-2003.

Wireless

The Department has a small number of laptops with wireless Internet access for use at offsite meetings and disaster communications access to the County's Emergency Management Information System.

The Public Library has a grant funded pilot project to provide the public with laptops for wireless access to the Internet at the San Fernando Library. The Department is currently working with ISD to secure the related wireless local area network prior to implementation. If this pilot is successful this concept will be expanded to other community libraries.

The Department is exploring the feasibility of providing wide-area wireless connectivity for three bookmobiles that serve rural parts of the County and network access to PDA's for staff use.

**GEOGRAPHIC INFORMATION SYSTEMS (GIS)**

The Public Library has implemented a geographic information system using ArcView software. This comprehensive system is used in the planning process for new and expanded library facilities and includes to Census demographic data and a wide variety of Departmental statistical data. The system is also utilized to map library services area boundaries and to conduct demographic analysis for the development of public service programs. A partial listing of the system's datasets include Transportation Analysis Zones with SCAP socio-economic information, public and private school data, 1990 and 2000 Census data, County Library locations, bookmobile stops and service statisitics, Library service area boundaries for Year 2000 and projected 2020 boundaries, and Thomas Bros. Data. In addition to providing a valuable management information tool for the Department the system can also be useful to other departments that provide municipal services to the unincorporated areas. The Public Library received a National Association of Counties (NACO) achievement award for the GIS system in 2002.

**WEB-BASED APPLICATIONS**

Web Catalog

The Library's catalog of materials is available as a web-based application on the Internet since 1998. The enhanced Web2 public access web catalog was implemented in July 2001, with the ability for customers to place requests on-line for County Library books, videos and other items. In 2002, the ability for customers to search several licensed on-line databases was added to the web catalog offerings. The Library will continue to explore adding additional functionality to the Web catalog, as well as adding online databases and other resources, as budgets permit.

Photo Identification System

The Department has implemented a centralized web-enabled photo identification system to allow the issuance of employee identification cards at Library headquarters and the five regional administrative office sites. The system utilizes a single client/server networked database that is controlled by the Department's Human Resources Division. The system reduces costs and loss of productivity since staff will only need to travel to Headquarters or the regional office closest to their work location to obtain a photo identification card.

Internet Management

The Library has implemented an Internet Management software program, which allows customers to make reservations, manages customer session time and printing, and which allows parents to decide if their

children's Internet sessions should be filtered. The patron reservation modules and the staff and administrator interfaces are web-enable applications.

Service Center

The Public Library currently utilizes the Service Center help desk system to record and track IT help calls. The Department plans to expand the system through the use of a web-based application which will provide end users the capability to search for a solution to problems in a knowledge database and submit/track trouble tickets.

Tutor.Com

Tutor.com, a web-based live homework help program, is offered at four County libraries to assist students grades 4 through 12 with their after-school studies. The program is offered through a grant from the California State Library.

## STORAGE AREA NETWORKS

The Department is piloting SAN technology using a four port SAN Fiber Switch from Qlogic, coupled with an Atto SCSI to Fiber bridge, connected to a 120GB Storage Dimension SCSI disk array. The SAN is managed by a Dell PowerEdge 2650 Server running the Qlogic SAN Manager. A Dell PowerVault Tape Library is used to backup the SAN. This configuration was chosen because of hardware and software compatibility and adaptability with our current hardware and software platforms.

The SAN has not been deployed into production due to the instability of the current storage disks array configuration. Also, we believe that the current version of the SAN software has stability problems. We are currently looking for ways to ensure the availability and integrity of the data. Possible solutions include on and off site redundancy and disaster recovery systems.

The Department plans to fully deploy the SAN by the end of 2003. The SAN will consolidate as much as 100GB of currently unmanaged storage and provide a centralized method of backing up and restoring data. This is contingent upon an acceptable redundancy system being in place in addition to availability of usable SAN-aware software.

The Department considers the SAN solution to be a critical part of its business continuity plan. With that in mind, we emphasized our need for data availability and required that all components be redundant. The SAN solution also includes a tape library. The tape library serves data archival needs and plays a part in any possible data recovery scenario. For minor data recovery events, such as those caused by user errors or virus infections, a real-time recovery method is desirable. Our experience with SAN has shown this to be an extremely useful feature. The ability for a SAN to go back to a point in time and restore specific data instantaneously is invaluable in terms of user productivity. SAN also benefits the data administrator because it provides the capability to more effectively manage data.

A County standard SAN solution would provide departments the capability to control a pool of storage that is guaranteed in terms of data access and recovery. This approach would reduce the high start up cost of SAN for individual departments.

## FY 2003-2004 OBJECTIVES

1.0 *Provide information technology infrastructure, support and maintenance to ensure access to library information.*

1.1 Initiate information technology infrastructure planning efforts for the new La Crescenta library in accordance with County standards.

1.2 Conduct analysis and complete information technology plans required for the proposed State Bond Act projects for the construction of East San Gabriel Valley, Acton, Lawndale, Diamond Bar, Duarte and West Hollywood.

1.3 Explore the feasibility of wireless data communications for providing remote access to the Department's integrated library system and the Internet for three bookmobiles serving rural areas of the County.

1.4 Manage the installation and acceptance testing of information technology and low voltage systems for the new East Los Angeles Library currently under construction. The facility is scheduled to be opened in the latter part of FY 2003-2004.

2.0 *Integrated Library System Replacement*

2.1 Replace 200 dumb terminals with Windows2000 workstations, in preparation for the new integrated library system.

2.2 Begin planning efforts for process of replacing the legacy system.

2.3 Begin identification of priorities for functionality in the new system.

2.4 Perform data cleanup activities on existing data files, to ensure consistency and integrity of data for the future data conversion to the new system.

2.5 Continue process of identifying and refining funding requirements for the replacement system.

3.0 *Improve the security of library materials*

3.1 Replace outdated electronic library material security detection systems at a minimum of ten community libraries.

4.0 *Improve the IT skills of library staff.*

4.1 Conduct a minimum of 40 training classes for library staff on core business applications and various modules of the integrated library system and the Internet management system in order to improve end-user skills and increase productivity.

4.2 Schedule training classes to improve the skills of library IT staff in areas such as data security, network management, Cisco switch configuration, and Intranet application development.

5.0 *Improve end user computing support*

5.1 Expand the use of the Service Center help desk program through the use of a Web based application which allows end users to search for a solution to problems in a knowledge database and submit/track trouble tickets.

6.0 *Enhanced Library Website*

6.1 Research web enhancement options, and consult with a group of end users.

6.2 Prepare design requirements for contract vendor.

6.3 Test and review re-designed web pages; submit changes to contract vendor.

6.4 Inform staff and other end-users, and implement enhanced web site.

# APPENDIX B:
# COUNTY OF LOS ANGELES
# WIRELESS LAN GUIDELINES

# Wireless LAN Guidelines

Version 1.4

**Reference:** Countywide Master Information Security Policy

**Developed by:** Remote Access Work Group, Mitigation of Cyber Terrorism

## 1.0 PURPOSE

The purpose of this document is to establish guidelines for deploying and operating Wireless Local Area Networks (WLAN) in Los Angeles County government organizations. WLAN components are relatively inexpensive and the benefits they provide easily justify their deployment. This paper provides organization leaders with the practical understanding of the factors related to the deployment and the operation of WLAN. The products based on IEEE 802.11 standards that have been certified by Wireless Ethernet Compatibility Alliance (WECA) for Wi-Fi (wireless fidelity) compliance are dominant in the industry. The focus is on the Wi-Fi compliant technologies. There are other WLAN technologies using infrared or other frequency spectrums. Other products are usually proprietary or they have not gained wide acceptance in the industry, and are not addressed in these guidelines. However, the practices recommended in these guidelines may be used to mitigate risk associated with other wireless technologies.

### 1.0.1 RELEASE NOTES AND HISTORY LOG

The content in this document will be periodically updated to reflect the changes in the County environment and to capture industry best practices as the technology and standards continue to evolve.

| DATE | NEW VERSION NUMBER | MODIFIED BY | DESCRIPTION OF CHANGE |
|---|---|---|---|
| 03/01/2003 | 1.2 | H. Kao (ISD) | 1) Content revisions were made. |
| 05/12/2003 | 1.3 | R. Pittman (CIO) | 1) Updated appendix E to add a sample of what information is required.<br>2) This final version was distributed at TSAB. |
| 08/08/2003 | 1.4 | R. Pittman (CIO) | 1) Added section 7.0.1 Submittal of Forms Procedure.<br>2) Added this history log in section 1.0.1.<br>3) The document date is no longer being generated automatically by Microsoft Word |
| | | | |

## 2.0 WIRELESS LAN DEPLOYMENT & OPERATION GUIDELINES

This Guideline was developed by Cyber Terrorism (CT) Security Engineering Team (SET) and is intended to address security issues related to remote network access and wireless network access in the County. This workgroup will produce recommendations that will fit the overall security framework, which will be formed based on the input of all workgroups within CT SET. The workgroup meetings are designed to provide a forum for collaboration among the team members, who are representatives from different organizations in the County. Through a consensus-driven process, the workgroup will produce recommendations and security guidelines that will help mitigate security risk in the County. The workgroup will identify security issues and determine their priorities according to the threat they present to the environment. The areas related to remote access and

wireless access in the environment that represent immediate threat to the County are addressed by the workgroup first.

As a part of the work under the Cyber Terrorism (CT) Security Engineering Team (SET), this paper emphasizes security risk mitigation related to WLAN. The aim is to provide a practical guide for WLAN by drawing from the proven practices and the knowledge gained in the industry. Each organization in the County, with the specific knowledge of its own business environment, will determine the appropriate capabilities for its requirements. As the industry evolves, WLAN standards and technology will continue to improve. These guidelines will be updated periodically to reflect the changes in the industry and to take into account the experience that is gained through the CT SET forum in the County.

## 3.0 WLAN OPENS UP YOUR IT ENVIRONMENT

There are three modes of WLAN operations. (1) WLAN Access Points (AP) are used to provide connection between LANs where physical infrastructure is not available. This type of networking is referred to as point-to-point (or point-to-multipoint) bridge mode of operation. (2) WLAN client stations communicate directly with each other on a peer-to-peer level. This type of networking is often formed on temporary basis, and is referred to as an "ad hoc" mode of operation. (3) The prevalent mode of WLAN operation is referred to as the "infrastructure" mode. In the infrastructure mode of operation the AP forms a bridge between the wired infrastructure and the wireless LAN. Client stations do not communicate on peer-to-peer basis. All communication between WLAN client stations or between WLAN client stations and any node on the wired network must go through the AP. AP's are not mobile; they are physically wired to the wired network infrastructure, hence the name infrastructure mode. The infrastructure mode is the dominant mode of operation in the County and, hence, the focus of these guidelines.

Functionally, WLAN may be used to either replace or to extend the LAN infrastructure. In most County organizations, WLAN are used in the infrastructure mode of operation. Whether you use it simply for extending connectivity beyond the physical boundary of your LAN, or for the flexibility of networking users without the constraint of a wire, WLAN expands your private network, and potentially expands your vulnerability to new kinds of security risk. The additional benefits you gain from WLAN must be balanced with the additional security burden you need to deal with. The policies and procedures governing the IT practices in your organization related to LAN deployments and operations should be the framework for determining the baseline requirements for WLAN. The current design guidelines, vendor selection process, and procurement procedures for network equipment also apply to WLAN. However, with WLAN, additional effort is required to cope with the risk associated with wireless communication.

WLAN presents new kinds of challenges to an organization. There is inherently less control over the integrity, reliability, and confidentiality of WLAN than you have with the wired LANs. The issues related to transmission contention, interference, and security risk associated with wireless communication require extra attention. Products based on the 802.11b standard dominate the industry today. 802.11b operates in the unlicensed 2.4GHz ISM (industry, scientific, medical) band as designated by FCC. Since it is not licensed, anyone may use it. Bluetooth, the short-range personal area network (PAN) technology also uses the 2.4GHz frequency spectrum. The FCC regulates the maximum transmission power and the bandwidth usage for each type of transmission in the ISM bands. For example, 802.11b uses a technique called direct sequence spread spectrum (DSSS) and Bluetooth uses a technique called frequency hopping spread spectrum (FHSS) for transmission. For each type of transmission, the FCC specifies the frequency range and the maximum power that is allowed.

The emerging 802.11a technology uses ISM band in the 5GHz range, which is treated the same way. No one has the right of way over the ISM frequency spectrum.

One characteristic of WLAN communication is that the AP's must broadcast their presence into the air regularly. This is a designed behavior of the AP according to the 802.11 standard. The management frames the AP's send out are referred to as beacons. Beacon frames are broadcasted without encryption. All client stations within the coverage area, whether they are legitimate clients or not, see the beacon frames broadcasted by the AP. The typical information the client can derive from the beacon frames are the service set identifier (SSID); the signal strength, the frequency channel, the MAC address, and even the location of the AP can be determined when a GPS is used. No hacking is required to learn about the details of an AP.

Between the AP and the client station, the reachable distance is proportionally increased with power (not to exceed 100mW internationally or 1W in the US) and inversely impacted by the speed of transmission. 802.11b may operate at 1Mbps, 2Mbps, 5.5Mbps, or 11Mbps. At 2Mbps and maximum power, the coverage distance is approximately 300 feet from the AP. However, industry experiments have shown that client stations equipped with high gain directional antennas may connect to WLANs over 25 miles away. One should realize that the physical boundary of the wired LAN, the AP, is where one's domain of control effectively ends. WLAN requires extra consideration in at least three areas: authentication, data encryption, and network integrity. Since the information is transmitted over an open medium, the data frames may be altered, authorized sessions may be hijacked, or imposters may impersonate the network to steal authentication credentials. Additionally, the types of denial-of-service attacks that might result from frequency interference, saturation, or jamming (intentional or unintentional) are difficult to prevent.

Despite the shortcomings, WLAN technology has gained wide acceptance across the industry. The emerging 802.11a (see Appendix A: WLAN Technology Primer) standard promises greater capacity and the 802.11i standard will provide solutions for many of the security problems associated with WLAN today. The technology is progressing and we need to move in alignment with the progress. One should recognize that the radio portion of the network is unsafe. The amount of security protection that is required will always depend on the service objectives. The current state of WLAN technology is neither good nor bad, it is only good or bad in the context of the business applications. The sensitivity, performance, and reliability of the business applications ultimately determine the design of the network infrastructure.

## 4.0 KNOW THE SECURITY REQUIREMENTS

IT security policy, explicit or implied, defines the rules that regulate how the County manages and protects its information and computing resources, and how to achieve security objectives. One of the policy's primary tasks for detecting signs of intrusion is to document important information assets and clarify the threats to those assets. When WLAN access points are introduced to a secure and trusted network in the County, additional considerations must be given to security issues. Specifically, there must be risk assessments to identify the impact WLAN access would have on the organization. Information assets must be inventoried. Hence the first priority is to examine the information resources that are worth protecting and then categorize them by the levels of security sensitivity.

Understand the consequences of security violations. Know the impact your organization has on the entire County when your network security is compromised. Considering the threat of cyber terrorism, what are the implications of a security breach in your network? If your network is connected to the County enterprise (data

centers and other departments) and is treated as a trusted entity by others, then a security breach in your network compromises the security of the entire enterprise.

WLAN security should be determined in the context of the organization's business. A practical solution will depend on the organization's ability to support it in its operating practices. How does one tell when there is a security violation? What types of features are embedded in the network infrastructure that will generate security alerts? Who in the organization will be responsible for enforcing the rules? What are the escalation procedures to resolve security problems in your organization? A sound security framework encompasses many policy and practice factors in addition to the features and functions embedded in the technology. WLAN will be an extension to your network and it will impose extra requirements for security because of the open nature of the technology.

## 5.0 KNOW THE BUSINESS DRIVERS

Think about the business reasons for WLAN before worrying about the technical issues such as coverage zones, frequency conflicts, and security vulnerabilities. Is WLAN for productivity gain, reducing cabling cost, or networking field service personnel? Once the business benefits and the technical challenges are understood, you can properly assess the merit of WLAN in your organization. What types of business functions in your organization warrant WLAN service? Where should you provide coverage and where should you not? What applications should be supported over WLAN? Who are the users of WLAN? What are their usage behaviors? Is there an alternative solution based on the existing wired infrastructure?

In general, when a wired connection is available it is always preferable to a wireless connection. With the security issues identified and other limiting factors such as reduced bandwidth availability, contention for a shared medium, and the unpredictable radio interferences, wireless solution should only be implemented where there is a legitimate business reason to do so. The cost of implementing a wired infrastructure alone is not a legitimate business reason for implementing WLAN except for temporary installations. There must be compelling business reasons for mobile computing.

Explore the deployment related questions after WLAN has been justified. Some basic questions are: What is the maximum number of users at a given service location? What is the maximum number of service locations required in a building? Are users from other County departments sharing the same service location or the same building? The reliability and security of WLAN services require extra planning and management effort because the transmission medium is open and unsecured, and the FCC does not license the transmission frequency.

## 6.0 DEPLOYMENT GUIDELINES

### 6.1.1 Considerations for Multi-tenant County Buildings

Special consideration must be given to the requirements in multi-tenant County buildings. In order to have WLAN reliability, integrity, and security there must be a joint effort among all departments sharing the same building to coordinate deployment and operation activities. Having one central IT management organization responsible for WLAN service in the building and accountable for enforcing a common usage policies will be the best way to proceed. Following are the main factors related to deployment.

### 6.1.2 Airwave usage

Within the County buildings the usage of airwaves shall be coordinated and managed by ISD or a central IT organization agreed to by all tenants in order to avoid unnecessary service degradation and exposure to security risk. If individual departments install their own AP's, they implicitly make claim of the shared airwave in the building without regard for the needs of other departments. Uncoordinated installation of WLAN's in a shared building will lead to excessive frequency interferences and degrade services for everyone. ISD or a central IT organization will control the airwave in the building. The "ad hoc" mode of WLAN operation will not be allowed. All WLAN operation shall be in the "infrastructure" mode only. Any unauthorized AP will be confiscated and removed from the building.

### 6.1.3 AP Management

ISD or an agreed upon central IT organization will manage the AP's in multi-tenant County buildings, and will have the responsibility to support WLAN communication for all departments in the building. AP devices that will be shared by multiple departments in the building will be deployed and operated to deliver a broader suite of functionalities than that of a single department. ISD or the central IT management organization, with clear responsibility for all AP's in the building, will help prevent unnecessary confusion among the departments. A central IT authority will coordinate the services and manage the ongoing operation more effectively.

### 6.1.4 Coverage Zone

WLAN coverage zones, "hot spots", in the multi-tenant County buildings will be determined according to the needs of every department in the building. The number of users in a given area and the number of coverage areas needed in the building must be determined in order to properly locate and configure the AP's. ISD or a central IT management organization shall consult each department in the building to identify their business drivers, applications, usage behaviors, and other designed requirements for the wired network infrastructures to determine a coverage zone that will serve all the tenants in the building.

### 6.1.5 AP Placement

The locations of AP placement will be determined according to the coverage zones required in the building. There should be special consideration for network security in selecting AP placement locations. Traditionally, firewalls are installed to defend the perimeters of the wired network, and they are monitored meticulously because the organization understands the potential risk outside. The organization considers the network outside the boarders unsafe because the outside environment is unpredictable and uncontrollable. Likewise, the environment outside the radio interface of the AP is unsafe; hence the installation of an AP implies opening up an entry point into the organization from a potentially unsafe territory. The placement location of an AP and the infrastructure behind it should be designed and managed to protect the interest of all tenants in the building as well as the security environment of the entire County.

### 6.1.6 AP Connection

The connection to the wired infrastructure in a multi-tenant County building should ensure that the AP has a path back to each department's LAN and application environment. In addition to ensuring the AP

supports connectivity to each department's backend environment, care must be given to the different needs of each department as dictated by their business drivers, application behaviors, bandwidth usage, security, etc. ISD or the central IT management organization shall consult all the departments in the building to understand their specific WLAN requirements in order to determine the proper connection point and the associated support infrastructure for the AP.

### 6.2.0 VLAN AND VPN FOR DISTRIBUTION

In a multi-tenant County building, all departments will share common AP's for WLAN communication. The distribution network behind the AP's is configured to deliver each user's traffic to the appropriate server environment where the department's applications reside. The application of interest for the particular user may be hosted locally in the building, in the ISD data center in Downey, in the department's own data center somewhere within the County, or outside the County's firewalls in the Internet. ISD or the central IT management organization needs to have broad capabilities and coverage for the entire County network in order to provide end-to-end transport service across geographically disperse locations. According to the unique requirements of each department, it might be necessary to support various levels of separation and protection for WLAN traffic. VLAN's will be used to separate user groups or departments in the building and VPN's in the Enterprise Network could be used in some situations to provide enhanced safeguard for transport to and from remote County locations. ISD or a central IT management organization, with the global view of interactions in the building, will create or recommend appropriate VLAN and VPN solutions for each tenant.

### 6.3.0 CLIENT DEVICE MANAGEMENT

Each department in a multi-tenant County building may purchase WLAN client devices independently. The devices, however, must be Wi-Fi compliant. For example, 802.11b standard based WLAN adapters for PDA's, Laptop PC's, or Desktop Workstations will be supported in the building. All client devices to be used in the building should be registered with ISD or the central IT management organization so they may be properly associated with the AP's in the building in order to support the functionality and security requirements.

#### 6.3.1 Authentication

In order to minimize security risk, all access attempts to the WLAN should be authenticated at the device level as well as the user level. At the device level, the device MAC address, SSID, device name, and the encryption key may be used collectively to verify the identity of the device. At the user level, user ID and password should be authenticated against an authentication database, which may be an enterprise directory or a RADIUS (Remote Access Dial-In User Services) server. A client device will be granted access to an AP only upon a combination of device and user authentication. ISD or a central IT management organization needs to maintain a common user directory database in order to determine the access level and service profiles of WLAN users in the building, and grant them appropriate services.

#### 6.3.2 Encryption

Each department in the multi-tenant County building might have different protection requirements for the data transmitted over WLAN. The transmission originates from WLAN might go through different

types of encryption and the actual end points of the encrypted tunnels might vary from one user to another. The vulnerability of WEP is well known in the industry and will not be sufficient for security protection generally. Additional capabilities such as user level authentication and dynamic encryption keys will be required to protect sensitive data. An encryption mechanism that provides a secured tunnel between the client station and the AP might be sufficient for some users, but others might require a VPN tunnel that extends all the way to the application servers, which may be a remote location across the Enterprise Network. ISD or a central IT management organization that has broad responsibilities across the County will be able to support a more comprehensive solution.

### 6.3.3 DHCP Server

After gaining access to the WLAN, the client devices need IP connectivity in order to communicate with the servers and applications, which might reside anywhere in the County. For security reasons, the IP subnet that is allocated to client devices should be different from the subnet allocated for AP management. The ability to manage address allocation based on unique user profiles gives IT management control over the WLAN traffic. The ability to manage address allocations, hence influencing routing and network reach ability, depends on the management of the DHCP (Dynamic Host Configuration Protocol) server. ISD or a central IT management organization that has global view of the entire networking environment should control the DHCP server and correlate its configuration with those in Switches and Routers in order enhance end-to-end connection service.

### 6.3.4 RADIUS Server

As a mechanism for managing user identities in the building, the profile of each WLAN user should be stored in an enterprise directory or a RADIUS server. Typically, a RADIUS server is used to authenticate users dialing into the network from remote locations. In addition to authentication services, it also provides the mechanism for controlling, monitoring, and accounting remote access activities. RADIUS serves the same functionalities for WLAN. ISD or a central IT management organization should manage identities of WLAN users on an enterprise directory or a RADIUS server and use RADIUS services to authenticate, monitor, audit, and log each client connection in order to ensure security.

### 6.3.5 Roaming Service

Within a shared building, WLAN users from different County departments may connect to the same AP. Since mobility in WLAN is limited to the Data Link Layer, WLAN clients need IP services in order to connect to the appropriate network resources. The design for roaming services will depend on a collection of other services: DHCP servers, DHCP relay on routers, RADIUS, cross-departmental directory database, etc. Both WLAN and the wired LAN infrastructure need to adapt to the special needs of the individual departments. The distribution network and the core network infrastructure behind the AP's must provide the necessary capabilities to support the different requirements. In addition to the transport requirements, authentication and encryption requirements must be addressed on multi-department basis. Since ISD has broad responsibilities for network infrastructures across the County, it will be in the best position to address the needs for multi-department roaming service.

## 6.4.0 CONSIDERATIONS FOR SINGLE-TENANT COUNTY BUILDINGS

County buildings that house a single tenant and are under the jurisdiction of a single management organization should be evaluated using the same criteria outlined for the multi-tenant situation above. The organization that is in charge of the building should coordinate and manage WLAN activities in the building. In order to have WLAN reliability, integrity, and security there should be one central IT management responsible for WLAN deployment and operation in the building. No business unit in the organization should install WLAN independently without collaborating with the central IT organization for the building. Following are identical factors as specified in the multi-tenant situation, except the task of implementation might be simpler because one department with one IT organization responsible for a smaller amount of services might encounter less obstacles in the process.

Airwave Usage
AP Management
Coverage Zone
AP Placement
AP Connection
VLAN and VPN for Distribution
Client Device Management
Authentication
Encryption
DHCP Server
RADIUS Server
Roaming Service

## 6.5.0 CONSIDERATIONS FOR NON-COUNTY BUILDINGS

A County organization that shares office space in a building that belongs to a non-County entity must observe the rules established by the building management. Even if no rule has been established for airwave usage in the building, the guidelines regarding airwave usage, AP management, coverage zone, AP placement, and AP connection, and roaming service must be evaluated using the same criteria as recommended above for the multi-tenant County buildings. Additionally, the design and management of the wired infrastructure that makes up the backbone for the AP's for the organization must meet County security requirements. The unique requirements for deployment and operation of WLAN to support an organization that shares non-County buildings need to be addressed on case-by-case basis with special consideration for the needs of other tenants in the building.

### 6.5.1 Configuration Guidelines

For practical reasons, the minimum configuration of WLAN infrastructure to support the appropriate level of security will be determined based on short-term, mid-term, and long-term requirements. Recognizing the realities of risk inherent in the current state of the technology, one should deploy WLAN products that serve today's needs and have the flexibility to adapt and grow as the technology continues to improve. While 802.11b technology has gained wide acceptance in the industry, developmental work continues in IEEE bodies and in the vendor communities to resolve the known problems and to enhance service capabilities. WLAN product life cycles are short. The following recommendations provide a baseline for County organizations to meet the minimum requirements for short-term, mid-term, and long-term security objectives. The configured parameters must be supported by the organization's operation practices as recommended in the next section. The ongoing management and operation of WLAN are integral parts of the solution. The following

configuration guidelines apply to any WLAN that directly or indirectly connects to the LAnet or the Enterprise Network.

### 6.5.2 Configuration for Short-term Requirements: Immediate implementation

1. No "ad hoc" mode is allowed, allow "infrastructure mode" operation only
2. Install AP's at a physically secured location
3. Provide basic device level authentication and encryption using WEP
4. Provide user level authentication
5. Unique SSID to distinguish WLAN
6. Create a unique name for each AP
7. Disable SSID broadcast
8. Enable a strong management password on each AP
9. Create separate IP subnets for AP management
10. Use DHCP server for client IP connectivity management
11. Restrict any unnecessary services: IP address and TCP port ranges
12. Create unique names to distinguish client devices
13. Use 128 bit WEP key for basic encryption services
14. Use MAC address filters on AP's to screen client devices.

### 6.5.3 Configuration for Mid-Term Requirements: Scheduled no later than 8/2003

1. Provide device level plus user level authentication and encryption
2. Provide dynamic encryption keys to overcome weakness of WEP
3. Provide 802.1x, EAP-TLS or equivalent
4. Provide dedicated LAN segment or VLAN for AP backbone
5. Force all AP's to pass authentication to a central RADIUS server
6. Use VPN, Firewall, and VLAN infrastructure to protect the wired network from WLAN

### 6.5.4 Configuration for Long-term Requirements: Scheduled for 8/2003 forward

1. Provide central directory database for authentication services
2. All AP's pass authentication to the central directory database
3. WLAN security infrastructure correlates to other network-based and host-based security mechanisms in the enterprise such as firewalls, routers, and applications to support the overall anti-cyber terrorism framework in the County.

## 7.0.0 OPERATION GUIDELINES

WLAN should not be treated as a fragmented installation. WLAN components should be added to the network management system, and the operating practices covering fault management, configuration management, performance management, and security management should be analyzed for compatibility and consistency. Integrating WLAN components into a unified management platform that supports network infrastructure for the organization will facilitate asset management as well as policy management and enforcement. Security policies can be enforced effectively only when there is visibility across the entire network – client to host and everything

in between. The airwave in WLAN frequency ranges should be managed as a part of the organization's assets. If the IT management organization controls who may connect to the wired infrastructure and the associated resources, it should do the same for WLAN. If the IT management organization partitions LAN traffic in order to protect sensitive data from potential risk, it should do the same with WLAN.

The management and operation of WLAN should be a natural extension to the network management system of the organization. The day-to-day operating practices play a critical role in creating WLAN security solutions. Monitoring and auditing functions should support the features and security attributes deployed in WLAN infrastructures as recommended in the previous section. The operation should continue to adjust and update support for the capabilities that are deployed for the short-term, mid-term, and long-term requirements. The following operation guidelines apply to any WLAN that directly or indirectly connects to the LAnet or the Enterprise Network.

### 7.0.1 Procedure for Submitting the Required Forms

The AP's that have connectivity into the County's enterprise environment shall be registered with ISD Data Security. ISD Data Security will maintain a database of AP's. The database will be used to periodically survey County facilities in order to prevent rogue AP's. An AP that is not in the database will be disconnected and confiscated. The AP database will also be used as a part of the CERT knowledge base for discovering network attacks in case of a cyber-terrorism event.

Registration by all departments will also ensure that the guideline configurations have been met and thereby the overall enterprise wide security is maximized.

Appendices D and E have Wireless LAN Security Checklist and Access Point Registration Form, respectively. Both documents are required to be submitted. The following procedure should be used for registering your wireless access points:

1. Review and adhere to the standards in appendix D
2. Complete the form in appendix E
3. The Chief Information Office, Chief Information Security Officer (CISO) will be overseeing this activity. Appendices D and E should be submitted to the following address:
   a) Send to Al Brusewitz, CISO, Chief Information Office, 9150 East Imperial Highway, Mail Stop 23, Downey CA 90242. For electronic document submission please send to: abrusewitz@cio.co.la.ca.us
   b) Also send a copy to Robert Pittman, Assistant CISO to the same address indicated in item a. For electronic document submission please send to: rpittman@cio.co.la.ca.us
4. ISD Data Security Division will require both documents for review and verification of compliance. Please complete appendices D and E and submit to:
   a) Send to Valerie Glass, Division Manager, ISD Data Security, 9150 East Imperial Highway, Mail Stop 25, Downey CA 90242. For electronic submission please send to: vglass@isd.co.la.ca.us

### 7.0.2 Operation for Short-term Requirements: To be implemented immediately

1. Register clients by user name, device name, and MAC address
2. Maintain an inventory of SSID, Client name, MAC address, and AP by building

3. Perform a risk assessment on AP's and associated resources
4. Monitor and capture patterns and trends of client-to-AP associations
5. Generate client association reports by client names and MAC addresses
6. Remove unauthorized AP's and unregistered clients from the network
7. Coordinate WEP key renewal every 30 days

### 7.0.3 Operation for Mid-Term Requirements: To be implemented no later than 8/2003

1. Manage profiles of WLAN users on a centralized RADIUS server
2. Centralized the management of AP configurations for all AP's
3. Support event notification on AP's – fault, threshold, log-in attempts, etc
4. Collect access and usage statistics on the RADIUS server
5. Generate audit logs and reports for security assessment
6. Generate security alerts on irregular events

### 7.0.4 Operation for Long-term Requirements: To be implemented 8/2003 forward

1. Manage all user profiles on an integrated directory database
2. AP's are included in the intrusion detection framework for the enterprise
3. Integrate WLAN management into the overall network management system
4. Keep up with FCC regulations on WLAN and the industry reports on security issues and the best practices to mitigate WLAN related security risk.

## 8.0 CONCLUSION

Know the benefits of WLAN in the context of the current state of the technology. Security standards are evolving and new products continue to emerge in the market place. Airwaves must be shared and unmanaged contention will degrade services for everyone. Product life cycles will be short. Know your security requirements in the context of the overall County requirements. Since the organization and network do not exist in isolation, compromising security also poses potential threat on other County organizations that connect to your network and trust it as a secured environment. The prudent approach is to deploy WLAN by following the mainstream practices in the industry today, and prepare network infrastructure with the flexibility to change.

Treat WLAN security as a component of the overall anti-cyber-terrorism initiative in the County. WLAN security is a part of the organization's IT security framework, which should include policies for resource allocation, prioritization, and protection. The enforcement of WLAN related security at different layers (application layer, operating system layer, network layer, and physical layer) should be an integral part of the organization's overall security framework. For example, the establishment of a central directory database for user identity management, VLAN and VPN for data confidentiality, and intrusion detection systems for network defense are inter-dependent mechanisms that collectively support policy enforcement.

Take the prudent approach and deploy practical WLAN solution without compromising security requirements. Justify WLAN based on your business drivers, and implement it based on the knowledge of the pros and cons outlined in these guidelines. Deploy it according to the short-term, mid-term, and long-term configuration guidelines. Update your network management system and operating practices to support it as you move from short-term to mid-term to long-term solutions.

## APPENDIX A: WIRELESS LAN TECHNOLOGY PRIMER

**IEEE 802.11:** IEEE 802.xx is a set of specifications for LANs from The Institute of Electrical and Electronic Engineers (IEEE). Most wired networks conform to 802.3, the specification for CSMA/CD based Ethernet networks or 802.5, the specification for token ring networks. 802.11 defines the standard for wireless LANs encompassing three incompatible (non-interoperable) technologies: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS), and Infrared. 802.11b uses DSSS to provide 11 overlapping channels across the 83 MHz within the 2.4 GHz frequency spectrums. Within the 11 overlapping channels, there are three 22 MHz non-overlapping channels. Since there are three channels that do not overlap, it is possible to use three AP's simultaneously to provide an aggregate data rate of the three non-overlapping channels. The emerging standard, 802.11a, uses 5 GHz spectrum to achieve data rates as high as 54 Mbps. 802.11a uses a type of frequency-division multiplexing called orthogonal frequency-division multiplexing (OFDM). The available bandwidth is divided into multiple data carriers. The data to be transmitted is then divided between the data carriers and treated independently from the others. The current expectation for finalization of 802.11a by the IEEE is mid 2003. Anther emerging standard is 802.11g, which is also expected around mid 2003. Product vendors will probably release 802.11g adapters and access points in late 2002 or early 2003. 802.11g standard is an extension to 802.11b. It will broaden 802.11b's data rates to 54 Mbps within the 2.4 GHz band using OFDM technology. Because of the backward compatibility, an 802.11b radio adapter will interface directly with an 802.11g access point (and vice versa) at 11 Mbps or lower depending on range.

The success and the continual momentum of WLAN technology is attributed to a nonprofit, vendor neutral organization known as Wireless Ethernet Compatibility Alliance (WECA). WECA provides a branding for the 802.11 technologies known as Wi-Fi (wireless fidelity). A Wi-Fi compliant device must pass the interoperability testing in WECA laboratory, and is assured compatibility with all other Wi-Fi certified products in the market.

**MAC (Medium Access Control):** In a WLAN network card, the MAC is the radio controller protocol. It corresponds to the ISO Network Model's level 2 Data Link layer. The IEEE 802.11 standard specifies the MAC protocol for medium sharing, packets formats and addressing, and error detection.

**CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance):** CSMA/CA is the principle medium access method employed by IEEE 802.11 WLANs. It is a "listen before talk": method of minimizing (but not eliminating) collisions caused by simultaneous transmission by multiple radios. IEEE 802.11 states collision avoidance method rather than collision detection must be used, because the standard employs half duplex radios—radios capable of transmission or reception—but not both simultaneously. Unlike conventional wired Ethernet nodes, a WLAN station cannot detect a collision while transmitting. If a collision occurs, the transmitting station will not receive an ACKnowledge packet from the intended receive station. For this reason, ACK packets have a higher priority than all other network traffic. After completion of a data transmission, the receive station will begin transmission of the ACK packet before any other node can begin transmitting a new data packet. All other stations must wait a longer pseudo randomized period of time before transmitting. If an ACK packet is not received, the transmitting station will wait for a subsequent opportunity to retry transmission.

**CSMA/CD (Carrier Sense Multiple Access/Collision Detection):** The LAN access method that is used in Ethernet. When a device wants to gain access to the network, it checks to see if the network is free. If it is not, it waits a random amount of time before retrying. If the network is free and two devices access the line at exactly

the same time, their signals collide. When the collision is detected, they both back off and each waits a random amount of time before retrying.

**ISM (Industry, Scientific, Medical) Band:** The frequency bands allocated for general usage without FCC license: 902 MHz to 928 MHz, 2.4 GHz to 2.4835 GHz, and 5.725 GHz to 5.850 GHz. For example, 802.11b and Bluetooth technology operate in the 2.4 GHz band, and 802.11a technology operates in the 5 GHz band.

**DSSS and FHSS:** Wireless LAN products are available in three different technologies – direct-sequencing spread-spectrum (DSSS), frequency-hopping spread-spectrum (FHSS) and infrared. DSSS and FHSS are spread-spectrum techniques that operate over the radio airwaves in the unlicensed ISM band (industrial, scientific, and medical). DSSS uses a radio transmitter to spread data packets over a fixed range of the frequency band. FHSS uses a technique by which the signal transmitted hops among several frequencies at a specific rate and sequence as a way of avoiding interference. WECA's focus is on the use of DSSS for 11 Mbps high rate wireless LAN communications.

**AP (Access Point):** A hardware device, or software used in conjunction with a computer, that serves as a communications "hub" for wireless clients and provides a connection to a wired LAN. An AP can double the range of wireless clients and provide enhanced security.

**Ad-Hoc Mode:** A client setting that provides independent peer-to-peer connectivity in a wireless LAN. An alternative set-up is where PCs communicate with each other through an AP. See AP and Infrastructure Mode.

**Infrastructure Mode:** A client setting providing connectivity to an AP. As compared to Ad-Hoc Mode where PCs communicate directly with each other, the clients that are set in Infrastructure Mode all pass data through a central AP. The AP helps mediate wireless network traffic in the immediate neighborhood and provides communication with the wired network. See AD-Hoc and AP.

**Roaming:** Moving seamlessly from one AP coverage area to another with no loss in connectivity. The 802.11 specifications do not stipulate a particular mechanism for roaming. Industry vendors choose their own algorithm for WLAN clients to make roaming decisions. AP sends out periodic management frames known as beacons. Beacons contain AP information such as service set identifier (SSID), support data rates, whether the AP supports frequency hopping or direct sequencing, and bandwidth capacity. The actions taken in the roaming process may differ from one vendor to another. Generally, the client may reinitiate a search for an AP in the same manner it started originally, or it may reference a table that was built during the previous association. Since the roaming techniques are vendor specific, roaming between AP's of different vendors may encounter compatibility problems or extended roam times.

**WEP (Wired Equivalent Privacy):** WEP data encryption is defined by the 802.11 standard to deter (1) access to the network by "intruders" using similar wireless LAN equipment and (2) capture of wireless LAN traffic through eavesdropping. WEP allows the administrator to define a set of respective "Keys" for each wireless network user based on a "Key String" passed through the WEP encryption algorithm. Access is denied to client stations that do not have the matching key string as coded in the AP.

**Bluetooth:** As a potential technology contender as well as a source of communication interference to 802.11 WLAN, Bluetooth is a short-range (about 10 meters) wireless technology operating in the same 2.4 GHz ISM band. Bluetooth wireless specification supports both data and voice applications. Operating in the same frequency spectrum, the radio uses spread spectrum, frequency hopping, and full-duplex signal at up to 1600

hops per second. The signal hops among 79 frequencies at 1 MHz intervals, which provides high degree of immunity to interferences.

In comparison to 802.11 WLAN, Bluetooth has much shorter range and lower throughput, which also means lower power consumption. The significantly lower power consumption makes it more ubiquitous than 802.11. For close-range personal area network, Bluetooth capabilities can be installed in personal digital assistants, cellular phones, pagers, printers, scanners, digital cameras, and home appliances - the original role was to replace short-range cables.

**Antenna:** Based on the coverage zone required, an antenna type can be selected for its radiation pattern. The radiation patterns may be omni-directional, bi-directional, or unidirectional. Omni-directional antennas are the vertical antennas that provide a radiation pattern like a donut shape, which is good for covering a large area horizontally. Vertically, the coverage provided by a vertical antenna is rather limited. Bi-directional antennas are the dipole antennas that provide a radiation pattern like a figure eight, which is good for covering corridors. Unidirectional antennas are the yagi or parabolic antennas that radiate in a single direction, which is good for setting up point-to-point links between buildings.

## APPENDIX B: SURVEY QUESTIONS RELATED TO WIRELESS LAN

1. Does your organization have WLAN?
2. Do you have 802.11b WLAN?
3. Do you have 802.11a WLAN?
4. Do you use WLAN in peer-to-peer mode (ad hoc mode) of operation?
5. Do you use WLAN in point-to-point bridge mode of operation?
6. How many WLAN access points do you have?
7. Do you use 128bit WEP on your WLAN access points?
8. How many WLAN users do you have?
9. Do you implement MAC filters on WLAN access points?
10. Do you implement user level authentication on WLAN?
11. Do you manage WLAN users on central RADIUS server for authentication?
12. Do you support dynamic encryption over WLAN?
13. Do you have an established operating procedure for WLAN?
14. Do you perform periodic audits on WLAN access points?
15. Do you have a dedicated VLAN for WLAN access points?
16. Do you have dedicated IP subnet for WLAN?
17. Do you support VPN over WLAN?
18. Do WLAN users access IT resources located locally?
19. Do WLAN users access IT resources in County data centers?
20. What applications WLAN users are using?
21. What client devices WLAN users are using?
22. Who are your WLAN product vendors?
23. Do you measure WLAN frequencies and coverage?

## APPENDIX C: POTENTIAL PROBLEMS ASSOCIATED WITH WIRELESS LAN

1. **"Rogue" Access Points**
   AP deployment in the organization without the IT department's knowledge is a problem. The relatively inexpensive WLAN components make it possible for many department staff, who traditionally depend on the IT department to supply them with technology, to buy AP's and client adapters themselves. WLAN devices are relatively inexpensive and little technical expertise is required to get them up and running in the factory default mode of operation. Unfortunately, the department staff can buy the devices under their budget authorities and can justify the benefits of WLAN, but they may not be aware of the security implications for the organization.

2. **AP's with factory default configuration**
   Many AP's are deployed with default configurations, which opens up avenues for un-authorized users to enter the network. There are results published in the Internet that majority of AP's are installed with minimum modifications to their factory default configuration. They either have not activated Wired Equivalent Privacy (WEP) encryption or simply use the default key as used by vendors coming out of the box. Even if there is no security concern for unauthorized users accessing the network, there are at least two problems that might result from such open access. Legitimate users might be denied of service because bandwidth is deliberately or unnecessarily consumed by unauthorized users, or hackers might use the network as a launching platform for cyber terrorism activities. Either could cause financial or legal challenges for the organization.

3. **Spoofing of client station MAC addresses**
   Network transmission based on 802.11 does not authenticate data frames. Every data frame has a source address but there is no mechanism to guarantee that the station sending the frame actually transmits the frame. There is no protection against forgery of the source address of the frame. Hackers can observe the MAC addresses of the stations in the network and use them for launching illegal activities. Requiring the users of the client stations to authenticate themselves before entering the network may mitigate this type of risk.

4. **Risk associated with traffic eavesdropping**
   Network transmission based on 802.11 does not protect data traffic against eavesdropping. The headers of data frames are transmitted in the clear, and are visible to anyone with a wireless network analyzer. WEP encryption protects the data to some extent but the management and control frames are not protected. The vulnerability of WEP is well publicized. The industry is actively working on standards to strengthen 802.11 securities and overcome the shortcomings of WEP. In the mean time, product vendors have introduced interim solutions such as using WEP in conjunction with key management protocols to change the encryption key on regular short intervals, which makes it impractical for attackers to decode. If WLAN is used to transmit sensitive data or to connect to internal networks, then stronger protection mechanism must be deployed at or closer to the data sources. A more comprehensive solution for authentication and encryption should be deployed for greater security.

5. **Service constraints**
   WLAN brings about new types of denial-of-service attacks, not necessary caused by malicious intent. Operating in the unlicensed frequency spectrum, no one has the right of way. The radio capacity can be overwhelmed by the traffic coming from the wired LAN or from excessive number of WLAN client stations trying to use the service at the same time. Or an attacker might disable the network by simply

sending a large amount of traffic on the same radio channel used by the AP. Other types of equipment (see Appendix A: WLAN Technology Primer) operating in the same frequency spectrum will interfere with WLAN integrity if they are in the same area. Perform regular auditing and traffic trending analysis will help the organization to plan and architect solutions to minimize service constraints.

## APPENDIX D: WIRELESS LAN SECURITY CHECKLIST

Month:_____ Date:_____ Year:_____

Organization Name: _____
Contact Information: _____
Responsible Manager:_____ Signature:_____

| SHORT-TERM REQUIREMENTS – To be implemented immediately | | |
|---|---|---|
| **CONFIGURATION** | **Mandatory** | **Recommended** |
| 1. "Infrastructure Mode" operation only. No "Ad Hoc Mode" is allowed | x | |
| 2. AP's are installed at physically secured locations | x | |
| 3. Provide basic device level authentication and encryption - WEP | x | |
| 4. Provide user level authentication | x | |
| 5. Create unique SSID to distinguish Wireless LAN | x | |
| 6. Create unique name for each Access Point | x | |
| 7. Disable SSID broadcast | x | |
| 8. Enable strong management password on AP's | x | |
| 9. Create separate IP subnet for AP management | x | |
| 10. Use DHCP server to manage and control client IP addresses | x | |
| 11. Restrict any unnecessary services: IP addresses and TCP ports | x | |
| 12. Create unique names to distinguish client devices | x | |
| 13. Use 128 bit WEP key for basic encryption services | x | |
| 14. Use MAC address filters on AP's to screen client devices | | x |
| **OPERATION** | | |
| 1. Register clients by user name, device name, and MAC address | x | |
| 2. Maintain inventory of SSID's, client names, MAC addresses, and AP's | x | |
| 3. Perform risk assessment on AP's and associated IT resources | x | |
| 4. Monitor and capture patterns and trends of client-to-AP associations | x | |
| 5. Generate client-AP association reports showing client names and MAC | x | |
| 6. Remove unauthorized AP's and unregistered clients from network | x | |

| | | |
|---|---|---|
| 7. Coordinate WEP key renewal every 30 days | | x |

| MID-TERM REQUIREMENTS – To be implemented no later than 8/2003 | | |
|---|---|---|
| **CONFIGURATION** | **Mandatory** | **Recommended** |
| 1. Provide device level and user level authentication & encryption | x | |
| 2. Provide dynamic encryption keys to overcome the weakness of WEP | x | |
| 3. Provide 802.1x, EAP-TLS or equivalent | x | |
| 4. Provide dedicated LAN segments or VLAN for AP backbone | x | |
| 5. Force all AP's to pass authentication to a central RADIUS server | x | |
| 6. Use VPN, Firewall, and VLAN infrastructure to protect wired network from WLAN | x | |
| **OPERATION** | | |
| 1. Manage profiles of WLAN users on a central RADIUS server | x | |
| 2. Centralize the management of configuration of all AP's | | x |
| 3. Provide support for event notification on AP's – fault, log-in attempts, etc | x | |
| 4. Collect access and usage statistics on RADIUS server | x | |
| 5. Generate audit logs and reports for security assessment | x | |
| 6. Generate security alerts on irregular events | | x |

| LONG-TERM REQUIREMENTS – To be implemented 8/2003 forward | | |
|---|---|---|
| **CONFIGURATION** | **Mandatory** | **Recommended** |
| 1. Provide central directory database for authentication services | | x |
| 2. All AP's pass authentication to central directory database | | x |
| 3. WLAN security infrastructure correlates to other network-based and host-based security mechanisms in the enterprise such as firewalls, routers, and | x | |

| | | |
|---|---|---|
| applications to support the overall anti-cyber terrorism security framework in the County | | |
| **OPERATION** | | |
| 1. Manage all user profiles on an integrated directory database | | x |
| 2. AP's are included in the intrusion detection framework for the enterprise | x | |
| 3. Integrate WLAN management in the overall network management system | x | |
| 4. Keep up with FCC regulations and industry reports on security issues and best practices to mitigate WLAN related security risk | | x |

## APPENDIX E: ACCESS POINT REGISTRATION FORM

**ACCESS POINT REGISTRATION**

| | AP Name & Type | MAC Address | IP Address | Power Out/ Channel | AP Location | Installation Date |
|---|---|---|---|---|---|---|
| 1. | Cisco 1200 | 001122334455 | 00.000.00.0 | 100mW/CH 6 | Telco Room L-40 3rd Floor 1000 Wireless Highway Signal, CA 90000 | 4-8-03 |
| 2. | | | | | | |
| 3. | | | | | | |
| 4. | | | | | | |
| 5. | | | | | | |
| 6. | | | | | | |
| 7. | | | | | | |

**Remarks:** New install. Will be using directional antennas.

**Contact person:** John Aironet
**Address:** 1012 West Temple Street
**City:** Los Angeles
**Telephone No.:** (000) 000-0000
**Email:** j_aironet@co.la.ca.us
**Date:** April 30, 2003

**Authorizing Manager/Department Information Security Officer (DISO) signature:**